Faculdade de Direito da Universidade Nova de Lisboa

PROTECÇÃO DE DADOS PESSOAIS NA INTERNET: O CASO DO "DIREITO A SER ESQUECIDO"

Vânia Sofia António Duarte

Dissertação de mestrado em Ciências Jurídicas Empresariais
Sob a orientação da Professora Doutora Maria Eduarda Barroso Gonçalves

Maio de 2014

Modo de Citação

Quanto às notas de rodapé optou-se pelo critério de referir a obra pela primeira vez com a referência completa e nas citações posteriores com referência abreviada.
Há uma bibliografia final que compila as monografias, os artigos, documentos consultados e jurisprudência consultada, com referências completas.

Lista de Abreviaturas

n.º: número
al.: alínea
pág.: página
CFUE: Carta dos direitos Fundamentais da União Europeia de 12 de Dezembro de 2007.
Directiva 95/46/CE: Directiva 95/46/CE relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de Outubro de 1995.
Directiva 2002/58/CE: Directiva relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, de 12 de Julho de 2002.
Directiva 2002/21/CE : Directiva relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (directiva – quadro), aprovada a 7 de Março de 2002.
LPDP: Lei da Protecção de Dados Pessoais - Lei n.º 67/98 de 26 de Outubro.
P.Reg: Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral), de 25 de Janeiro de 2012 – Documento COM(2012) 11.

Pro forma

Para efeitos de contagem de caracteres, indica-se que a presente dissertação tem 101.274 caracteres.

Resumo

A presente dissertação tem como objecto de estudo o direito a ser esquecido, um novo direito do titular dos dados proposto no Regulamento Geral de tratamento de dados, para reforçar o controlo dos dados pessoais pelo seu titular.

Analisar-se-á a protecção de dados pessoais na internet, nomeadamente, alguns cenários de tratamento de dados pessoais na Internet e o regime aplicável (directiva 95/46/CE e directiva 2002/58/CE).

Palavras chave: direito a ser esquecido, tratamento de dados, dados pessoais.

Abstract

The present dissertation has as object of study the right to be forgotten, a new right for increase the control of subject over their data.

It's analyzed the data protection on Internet, especially, some scenarios of processing and the regulation applicable to it (directive 95/46/CE and directive 2002/58/CE).

Key words: right to be forgotten, processing, personal data.

Índice

INTRODUÇÃO

Actualmente a Internet é uma realidade presente na vida de cada pessoa. A Internet é como um novo "mundo" que permite experiências e facilidades aos utilizadores da Internet.

Se outrora tínhamos que ir a uma biblioteca procura informações sobre um determinado assunto, agora basta pesquisarmos uma palavra – chave num motor de busca para nos aparecer uma panóplia de páginas *Web* relacionadas com o tema e com tantas apresentações e interpretações do tema, consoante o número de páginas apresentadas. Além disso, permitiu às pessoas a aquisição de produtos ou a adesão a serviços, com preços e condições especiais, dado o meio utilizado; a possibilidade de manifestarem as suas opiniões e preferências através de *blogs*.

Com o surgimento das redes sociais, foi possível o contacto com amigos de longa data, conhecer novos amigos e comentar e partilhar vídeos e musicas.

Até influenciou o contacto entre os cidadãos e o Estado, permitindo que aqueles tenham acesso a serviços através das plataformas das várias organizações do Estado na *Internet* (por exemplo: Finanças e Segurança Social).

No entanto se por um lado a evolução tecnológica e a globalização transformaram o acesso a informações e a interacção entre pessoas e entre estas e o Estado, por outro lado também criaram ameaças à privacidade destas, uma vez que permitem recolher e tratar um grande fluxo de dados pessoais. A partilha de informações pelos próprios utilizadores de *Internet* e o seu armazenamento em *cloud*[1] colocam em risco o controlo desses dados pelos próprios titulares.

Face a este contexto digital a Comissão Europeia e o Parlamento Europeu propuseram um novo regime de protecção de dados, visando substituir a directiva 95/46/CE. Este novo regime terá a forma de Regulamento, procurando harmonizar a matéria da protecção de dados em todos os Estados – Membros.

[1] Armazenamento em Servidores à distância, designadamente, em outros Países, que permitem que a informação esteja acessível em qualquer parte do mundo, sem que a pessoa tenha que levar dispositivos móveis de armazenamento consigo.

Uma das soluções propostas é o direito a ser esquecido (ou direito ao esquecimento) que visa permitir às pessoas singulares um controlo efectivo sobre os seus dados pessoais, designadamente, a possibilidade de apagarem informações sobre si e quaisquer referências a elas.

O objectivo deste trabalho é estudar este novo direito, apresentando o regime proposto, compará-lo com o regime anterior e a sua aplicação prática, incluindo neste ponto as dificuldades técnicas da sua aplicação.

O estudo deste direito justifica-se pela importância que tomará caso a proposta da Regulamento seja aprovada. Sempre que uma pessoa comenta uma notícia ou fotografia, quer seja numa rede social ou outra página *Web*, partilhe fotografias ou relate as suas actividades diárias ou acontecimentos sobre a sua vida, essas informações ficam permanentemente registadas. Qualquer pessoa pode copiar uma fotografia, comentário ou relato e guardá-la no seu computador. O mesmo ocorre entre páginas *Web*, que fazem referência a outras páginas ou ao seu conteúdo. Por exemplo, uma fotografia de uma pessoa pode ser apresentada em múltiplas páginas *Web*, podendo ainda ser guardada num computador, *pen* ou outro dispositivo móvel de armazenamento. Imaginando que essa fotografia mostra um acontecimento embaraçoso da pessoa em questão, aquela não terá possibilidade de esquecer o acontecimento, uma vez poderá encontrar essa fotografia nalguma página *Web* e nem a população em geral esquecerá, dado que a informação está sempre acessível.

Se anteriormente a esta revolução informática, um acontecimento podia ser esquecido com o decorrer do tempo, a manutenção das informações na rede, não o permitem. O direito a ser esquecido visa permitir um *reset* no historial do titular dos dados, um novo começo para aquela pessoa.

PLANO DE EXPOSIÇÃO

De modo a desenvolvermos o tema a que nos propusemos, no primeiro ponto analisaremos alguns cenários em que dados sobre utilizadores de Internet são recolhidos e tratados. Procuraremos analisar a qualificação desses dados como dados pessoais à luz da directiva 95/46/CE, que actualmente regula a protecção de dados pessoais, uma vez que dessa qualificação depende a aplicação a esses cenários dos princípios e regras respeitantes ao tratamento de dados pessoais.

No segundo ponto, realizarei o enquadramento histórico da evolução da protecção de dados pessoais, de forma a explicitar as preocupações subjacentes à protecção de dados pessoais.

No terceiro ponto, realizarei o enquadramento jurídico do tratamento de dados pessoais, analisando o actual regime de protecção de dados aplicável a dados pessoais e referirei as soluções apresentadas na proposta de regulamento para o tratamento de dados. Neste ponto pretendo analisar os princípios aplicáveis ao tratamento de dados pessoais e os direitos dos titulares dos dados face ao responsável pelo tratamento previstos na directiva 95/46/CE e directiva 2002/58/CE e as soluções propostas do regulamento geral para adaptar o regime de protecção de dados pessoais às novas tecnologias e reforçar os direitos dos seus titulares.

Por fim, no último ponto, analisarei o regime do direito a ser esquecido proposto, estudando o contexto para a criação deste direito, a aplicação prática do direito e as suas dificuldades e a sua consagração no domínio penal.

I. Tratamento de dados pessoais na Internet

Todos os dias milhões de pessoas acedem à Internet para pesquisarem informações, comprar produtos, contratar serviços, verificar o correio electrónico, consultar bases de dados e redes sociais, partilhar experiências em salas de conversação, *blogs* ou outras páginas *Web*. Todas estas actividades deixam pegadas electrónicas que podem ser recolhidas a tratadas por várias agentes presentes na Internet.

Essas pegadas electrónicas são informações passíveis de identificar o utilizador da Internet, tendo sido crescente a preocupação dos utilizadores da Internet quanto à preservação da sua privacidade. Por exemplo, de acordo com um estudo da Comissão Europeia[2], 25% dos cidadãos europeus inquiridos qualificaram os websites que visitam como informações pessoais, tal como as suas actividades diárias (25%), experiência profissional (30%) e fotografias (48%).

De acordo com o artigo 2º al.b) da directiva 95/46/CE podemos qualificar como tratamento de dados pessoais "qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados (…)". Logo, a recolha, organização e difusão, entre outras operações são consideradas tratamento de dados pessoais, se incidirem sobre informações qualificáveis como dados pessoais.

1. Conceito de dados pessoais

Segundo o artigo 2º al.a) da directiva 95/46/CE são dados pessoais "qualquer informação relativa a uma pessoa singular identificada ou identificável." Sendo que não só se qualifica como dado pessoal uma informação que directamente identifica uma pessoa, mas também o conjunto de informações que possam identificar a pessoa, nomeadamente " um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

[2] "Attitudes on Data Protection and Electronic Identity in the European Union", Eurobarometer Especial 359, publicado em Junho de 2011, pag. 12. Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

A LPDP, a lei que transpôs a directiva 95/46/CE para a Ordem Jurídica Portuguesa, apesar de no seu artigo 3º al.a) ter adoptado uma definição idêntica à da directiva, especificou que a informação pode ter qualquer suporte, nomeadamente som e imagem.

Assim podemos considerar como dados pessoais o nome, a morada, o número de telefone, a filiação partidária e sindical, o historial médico, os extractos bancários, e no âmbito da Internet, há que qualificar como dado pessoal o endereço electrónico, o IP, os dados de tráfego, os dados de localização.

O endereço electrónico (*email)* é como a morada do utilizador de Internet no serviço de correio electrónico. Qualquer pessoa que o queira contactar pode enviar uma mensagem para esse endereço. O endereço electrónico é composto de dois elementos: o primeiro antes do símbolo arroba (@) que é a identificação do utilizador do correio electrónico e o segundo elemento depois do símbolo arroba (@) o nome do fornecedor de serviços de Internet (*Internet Service Provider* - ISP). Assim que o ISP recebe uma mensagem identifica o utilizador, reencaminhando a mensagem para ele.

O IP é um endereço numérico que identifica o computador quando ligado à internet, que consiste em quatro blocos de até três algarismos, entre 0 e 255. É este conjunto de números que identifica o utilizador, sendo por isso considerado dado pessoal. Sempre que enviamos um *email*, acedemos a uma página - Web ou realizamos um download, o nosso IP é transmitido ao servidor, identificando - nos na internet.

Os endereços IP são geridos internacionalmente pela *Internet Corporation for Assigned Names and Numbers*[3], que são posteriormente atribuídos a um *Regional Internet Registry*, uma organização responsável pela atribuição do IP numa área geográfica delimitada. Na Europa é o *Réseaux IP Européens Network Coordination Center*[4] (RIPE NCC). O RIPE NCC faculta os endereços IP a *Local Internet Registries,* que são fornecedores de acesso à internet, que por sua vez os atribuem aos utilizadores de internet, mediante um contrato, ou gestores de redes locais que atribuem um IP a cada computador ligado à rede privada que gerem.

[3] https://new.icann.org/es
[4] http://www.ripe.net/lir-services/ncc

Os dados de tráfego são os dados recolhidos para efectuar o envio da comunicação ou para efeitos de facturação. De acordo com o considerando 15 da Directiva 2002/58/CE podem ser considerados dados de tráfego os relativos "ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedido ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação."

Os dados de localização são dados referentes à localização do utilizador, que segundo o considerando 14 da directiva 2002/58/CE podem incidir sobre " a latitude, a longitude e a altitude do equipamento terminal do utilizador, sobre a direcção de deslocação, o nível de precisão da informação de localização, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização."

As sequências de *clicks* (*clickstream*) são as ligações percorridas pelo utilizador, as hiperligações que segue e as páginas – Web a que acede que ficam guardadas no servidor particular, caso seja intranet, ou no servidor do *Internet Service Provider*.

Os dados recolhidos automaticamente na Internet são muitas vezes dados técnicos referentes à ligação à Internet ou inicio ou fecho da sessão numa determinada página *Web*, mas também podem ser sobre preferências e escolhas do utilizador, sem directamente se referirem à sua identificação. Há que analisar então se a entidade ou pessoa singular que recolheu os dados pode identificar o utilizador a partir desses dados, como referido no considerando 26 da directiva 95/46/CE. Este considerando ressalva que para uma pessoa ser identificável é necessário considerar "o conjunto de meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa (…)".

Concluindo, o critério a utilizar é se a informação recolhida identifica ou pode identificar o utilizador da Internet. Como veremos nos números seguintes, existem vários cenários de recolha e tratamento de informações sobre pessoas na Internet, mas só são qualificados como tratamento de dados pessoais e sujeitos às disposições legais

sobre esta matéria se as informações recolhidas forem qualificadas como dados pessoais.

2. Tratamento de dados pelos vários agentes presentes na Internet

São vários os agentes presentes na Internet com possibilidade de recolher e tratar dados pessoais. Alguns deles são as entidades com quem o utilizador tem que interagir contratando os seus serviços para aceder à Internet. São eles: os operadores de telecomunicações com os quais os utilizadores contratam os pacotes de Internet e telefone; os Fornecedores de Acesso à Internet (IAP) que fornecem ao utilizador, mediante um contrato, uma ligação TCP/IP[5], permitindo-lhes o acesso à Internet; os Fornecedores de Serviços de Internet (ISP) que prestam os serviços de internet, nomeadamente, o acesso ao correio electrónico e o alojamento de páginas Web. Muitas vezes o ISP e o IAP são a mesma entidade, no entanto pelas especificidades técnicas das suas funções há que separá-los para melhor compreensão.

Cada um destes agentes regista informações sobre o utilizador, assim que este acede à Internet. Os operadores de telecomunicações registam o IP e os dados de tráfego para efeitos de facturação; o ISP para além de registar o IP, recolhe também os dados sobre a sessão, ou seja, data e hora do *log in* e do *log out*,; o IAP ou o gestor de redes locais[6] registam o IP do utilizador, a data e hora de acesso, para além de conservarem um ficheiro log de cada utilizador.

Os ficheiros log registam informações sobre a ligação à internet, nomeadamente a data, duração, o tipo de utilização da rede (uso de correio electrónico, pesquisa…), as páginas Web visitadas e os destinatários de mensagens que enviadas.

---

[5] A ligação TCP/IP é um conjunto de protocolos para a comunicação entre uma rede de computadores, derivando o seu nome de dois protocolos - *Transmission Control Protocol* e *Internet Protocol.* Esta ligação permite o envio e recepção de pacotes de informação na rede.

[6] O gestor de uma rede fechada de computadores ligada à Internet atribui o IP a cada um dos computadores da rede, conhecendo desse modo o IP correspondente a cada utilizador da rede. Ver: Grupo do artigo 29º, "Privacidade na Internet – Uma abordagem integrada da EU no domínio da protecção de dados em linha-", de 21 /11/2000, p. 9. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_pt.pdf#h2-15

Além disso, cada hiperligação seguida pelo utilizador é registada. Quando pesquisamos num *browser* uma informação, o nosso IP, a palavra – chave utilizada no *browser*, a data e hora, a página anteriormente visitada e até a língua falada, são registados no servidor HTTP[7], pelos ISP.

O IAP ao contratar com o utilizador de Internet o seu acesso atribui-lhe um IP, o qual regista num ficheiro juntamente com os dados do utilizador e data e hora da atribuição[8]. Pelo que os dados que o IAP recolhe cada vez que o utilizador acede à Internet podem ser associados ao nome do utilizador, identificando-o.

O mesmo acontece com o ISP que ao contratar com o utilizador os seus serviços fica com a sua identificação.

Portanto é de concluir que os dados tratados pelo IAP ou Gestor de Redes Locais e o ISP são dados pessoais e portanto o tratamento dos dados pessoais realizado por estes agentes está sujeito às disposições legais nesta matéria.

3. Páginas Web

A Internet disponibiliza páginas *Web*, plataformas e aplicações que veiculam um leque variado de informações e possibilitam o acesso a vários serviços a um indeterminado número de pessoas. Para tal os utilizadores da Internet só têm que pesquisar na página de navegação (*Browser*) uma palavra – chave relacionada com o tema que procura.

Qualquer pessoa singular ou jurídica que tenha um computador pode disponibilizar páginas *Web*, bastando para tal contratar com um ISP o alojamento das mesmas no seu servidor.

---

[7] Servidor http pode ser um programa de computador (software) ou um computador (hardware) responsável pela transferência de dados. No primeiro caso é um programa instalado no computador responsável por recepcionar pedidos do utilizador de internet no browser e responder-lhe. Neste caso o servidor está vocacionado para a navegação na Internet. No segundo caso, sendo o computador o servidor em si, visa hospedar páginas Web garantindo que estão disponíveis para todos na Internet. Ver: http://www.webdevelopersnotes.com/basics/what_is_web_server.php

[8] Documento de trabalho do Grupo do Artigo 29ª, sobre privacidade na Internet, pág.9.

O titular de uma página *Web* pode recolher e tratar informações sobre os utilizadores da Internet em diferentes casos.

Primeiro, pode tratar os chamados dados sobre as visitas, registando o IP, o URL da página anteriormente visitada por ele, data e hora a que acedeu e os nomes e dimensões dos ficheiros a que acedeu ou descarregou.

A recolha destes dados não significa que o titular de uma página *Web* esteja a realizar um tratamento de dados pessoais, pois se não puder identificar o utilizador a partir dos dados que detém, esses dados não são considerados dados pessoais. Em cada caso concreto há que analisar se o titular de uma página *Web* recolhe informações sobre o utilizador através de outros mecanismos de recolha de dados, como por exemplo *cookies*, possibilitando dessa forma identificar o utilizador.

Segundo, quando a página dispõe de formulários de adesão a serviços ou de compra de produtos ou inquéritos. Nestes casos o utilizador da Internet dispõe dos seus dados pessoais, enviando-os para o titular da página e por isso há um tratamento de dados pessoais.

Terceiro, o próprio conteúdo de uma página *Web* pode ser considerado tratamento de dados, quando contenha dados pessoais de alguma ou algumas pessoas.

O Tribunal de Justiça da União Europeia teve oportunidade de se pronunciar sobre a aplicação da directiva 95/46/CE ao tratamento de dados pessoais numa página *Web* no Caso Lindqvist[9].

O Tribunal considerou, neste caso, que as operações de compilação, organização e de difusão de dados pessoais, nomeadamente nome, número de telefone, passatempos e condições de trabalho numa página de Internet são qualificáveis como tratamento de dados pessoais. Além disso considerou que os meios necessários para alojar a página Web no Servidor Web e disponibilizar a página às pessoas ligadas à Internet eram meios

[9] Processo C-101/01, de 6 de Novembro de 2003. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1400069636627&uri=CELEX:62001CJ0101

automatizados, subsumindo-se desta forma na definição de tratamento de dados pessoais constante no artigo 2º al. b) da directiva.

3.1. Redes Sociais

As redes sociais são também uma realidade actual na Internet. São plataformas que permitem aos seus utilizadores partilharem experiências, fotografias, vídeos e música, trocarem mensagens e usarem um leque de aplicações (por exemplo: serviços de comunicação social, de emprego, etc).

Os utilizadores constroem perfis digitais com o seu nome, número de telefone, cidade onde moram, local de trabalho, fotografias, amigos, actividades diárias, gostos pessoais, etc pelo que aos responsáveis por estas plataformas é possível compilar e tratar um elevado número de informações sobre os utilizadores.

3.2.Cookies

Os *cookies* são ficheiros com um conjunto de informação padronizado que regista qualquer informação que a entidade que o instalou pretenda, nomeadamente, o endereço IP, as hiperligações seguidas na Internet e as escolhas e preferências do utilizador. Em regra, os cookies só podem ser lidos por quem o implantou.

Os *cookies* podem ser enquadrados em diferentes categorias:

- *cookies* do próprio ou de terceiros, quando instalados pelo titular da página *Web* visitada pelo utilizador ou instalados por terceiros, responsáveis por tratar esses dados, através das páginas *Web*;

- *cookies* permanentes ou temporários, consoante fiquem armazenados no equipamento terminal do utilizador até uma data de expiração determinada ou sejam eliminados assim que o utilizador encerra o motor de pesquisa (*browser)*;

- *cookies* técnicos são aqueles que permitem a utilização de uma página *Web*, aplicação ou plataforma por parte do utilizador, possibilitando-lhe comprar produtos numa página *Web*, visionar vídeos e ouvir música ou preencher um formulário de inscrição para um concurso.

- *cookies* de personalização, que permite que as páginas *Web* e aplicações funcionem com critérios definidos pelo usuário;

- *cookies* comportamentais que permitem analisar o comportamento do utilizador nas páginas *Web* a que estão associados;

- *cookies* de publicidade que permitem gerir os espaços publicitários na página *Web;* e

- *cookies* para publicidade comportamental que visam criam um perfil do utilizador para lhe mostrar publicidade personalizada.

Os *cookies* proporcionam ao utilizador da Internet várias experiências. A sua instalação facilita a navegação do utilizador na internet e o acesso a serviços *online*. Por exemplo, permitem que a página *Web* reconheça o utilizador quando acidentalmente tenha encerrado a sessão; possibilita que quando o utilizador aceda uma segunda vez à página *Web* esta lhe seja apresentada na língua falada por ele, com imagens e cores escolhidas por ele e até com uma nota de boas vindas a si dirigida; e ainda a detecção de erros no envio das comunicações electrónicas.

Os *cookies* têm finalidades úteis e necessárias para os utilizadores da *Internet*, pelo que a sua instalação para fins legítimos é permitida. Todavia, dependendo da codificação dos *cookies* eles podem representar riscos para a privacidade dos utilizadores de *Internet.*

Os *cookies* podem ser codificados para transmitirem informações sobre os utilizadores de *Internet* que superam as finalidades para que foram instalados ou até instalados sem conhecimento do utilizador.

As informações recolhidas através de cookies podem ser utilizadas para criar perfis dos utilizadores e utilizadas em marketing, publicidade ou para outros fins estabelecidos pelas entidades que os criaram.

As informações obtidas através de *cookies* que possam identificar o utilizador de internet são qualificadas como dados pessoais e por isso o seu tratamento está sujeito às disposições das directivas 95/46/CE e 2002/58/CE.

4. Motores de Pesquisa

Os motores de pesquisa (*search engine)* são programas informáticos que se destinam a fornecer ao utilizador de *Internet* uma lista de resultados consoante a palavra – chave pesquisada pelo utilizador. Facilitam a navegação na *Internet* e o acesso dos utilizadores à informação, uma vez que fazem a ligação entre o utilizador da *Internet* e as páginas *Web*.

Para que seja apresentada uma lista de resultados ao utilizador, o motor de pesquisa armazenam informações das páginas *Web* através do chamado *Web crawler*, um programa informático que pesquisa páginas *Web* e todas as suas ligações. Posteriormente essas informações são registadas e organizadas pelos programas de indexação. É possível ainda aos motores de pesquisa guardarem parte ou totalidade das páginas agregadas em memórias *cache*[10], permitindo-lhes apresentar essas páginas quando eles já não estão disponíveis na rede.

Os motores de busca ao analisarem a *Internet* através dos programas de indexação recolhem e registam um elevado número de informações, incluindo dados pessoais.

O Tribunal da União Europeia pronunciou-se sobre o tratamento de dados pessoais pelos motores de pesquisa no Processo C-131/12[11] e considerou que a actividade dos motores de pesquisa pode ser qualificada como tratamento de dados, porque armazena

[10] Cache é um dispositivo para acesso rápido a uma página *Web* ou base de dados. Permite ao motor de pesquisa apresentar um página *web* já visitada com mais rapidez, não tendo que fazer o seu download, o que seria mais demorado. Ver: http://www.tecmundo.com.br/navegador/201-o-que-e-cache-.htm

[11] Processo C-131/12, de 13 de Maio de 2014, do Tribunal de justiça da União Europeia. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62012CJ0131.

dados pessoais, disponíveis nas várias páginas *Web*, organizando-os e apresentando-os sob a forma de lista aos utilizadores da i*nternet.*

O facto de os dados pessoais serem recolhidos juntamente com outras informações disponíveis, sem existir uma recolha específica desses dados, não inviabiliza essa qualificação, porque como se pode ler no parágrafo 28 do acórdão: "Na medida em que estas operações estão explícita e incondicionalmente referidas no artigo 2.°, alínea b), da Diretiva 95/46, devem ser qualificadas de «tratamento» na aceção desta disposição, independentemente de o operador do motor de busca efetuar as mesmas operações também com outros tipos de informação e não as distinguir dos dados pessoais."

O mesmo ocorre com o facto de os dados não serem alterados pelos motores de pesquisas, apenas servindo estes de intermediários entre o utilizador e a página *Web*, porque segundo o tribunal " decorre da definição contida no artigo 2.°, alínea b), da Diretiva 95/46 que, embora a alteração de dados pessoais constitua, é certo, um tratamento na aceção dessa diretiva, em contrapartida, as demais operações aí referidas não carecem minimamente que esses dados sejam alterados."[12]

Concluindo, os motores de busca no âmbito da sua actividade realizam operações que podem ser qualificadas como tratamento de dados, e uma vez que são eles que definem os meios e as finalidades da sua actividade são considerados responsáveis pelo tratamento, devendo respeitar os princípios e regras aplicáveis ao tratamento de dados e permitir aos utilizadores da *internet* o exercício dos seus direitos, segundo a directiva 95/46/CE.

[12] Processo C-131/12, parágrafo 31.

II. Enquadramento histórico

1. "The right to Privacy"

A preocupação com a protecção da vida privada ganhou relevância no séc. XIX quando Samuel Brandeis e Louis Warren, em reacção ao uso de informações pessoais e fotografias pela imprensa escrita, publicaram na *Harvard Law Review* o artigo "The Right to Privacy". Nesse artigo formulam pela primeira vez o "right to be left alone", que traduzido literalmente, é o direito a ser deixado em paz. Esse direito consistia em o indivíduo conduzir a sua vida livremente, sem ingerências externas, permitindo-lhe manter uma esfera de segredo sobre a sua vida privada e prevenindo a má reputação e a discriminação social.

De acordo com os autores, cada indivíduo tem o direito de determinar quando revela os seus pensamentos, sentimentos e emoções, não podendo ser obrigado a fazê-lo. Mesmo no caso de o indivíduo decidir revelar essas informações, estas continuam na sua disponibilidade, podendo controlar a publicidade dada às mesmas[13].

Este direito é formulado, pelos autores, como direito geral de personalidade, garantindo protecção às variadas dimensões da personalidade que até então não eram protegidas[14].

Os tribunais americanos só reconheceram o "right to privacy" em 1905 no caso Pavenish v. New England Life Insurance Co. Neste caso, Paolo Pavenish instaurou uma acção contra New England Life Insurance Co, por esta ter utilizado uma fotografia, sem o seu consentimento, numa campanha publicitária. O tribunal condenou a empresa e o fotógrafo que cedera a imagem, ao pagamento de uma indemnização, pela violação do "right to privacy".

---

[13] BRANDEIS, LOUIS D., WARREN, SAMUEL D., "The Right to Privacy", Harvard Law Review, Vol. IV, N.º5, Dezembro 1890. Texto disponível online em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

[14] CASTRO, CATARINA SARMENTO E, " O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro", página 3. Disponível em: http://www.estig.ipbeja.pt/~ac_direito/CatarinaCastro.pdf

O primeiro instrumento jurídico internacional que consagrou o direito à reserva da vida privada foi a Declaração Universal dos Direitos do Homem, em 1948. No seu artigo 12º é referido que "Ninguém sofrerá intromissões arbitrárias na sua vida privada…".

Na Europa, o direito à reserva da vida privada foi consagrado pela primeira vez na Convenção Europeia dos Direitos do Homem consagrou, em 4 de Novembro de 1950. No seu artigo 8º n.º1 pode-se ler que "toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência."

2. A revolução informática e a génese dos regimes dos regimes de protecção de dados pessoais

O século XX trouxe uma revolução ao nível dos meios de comunicação e do acesso à mesma pela população. Com o nascimento do Eniac (*Electronic Numerical Integrator and Computer),* a 14 de Fevereiro de 1946, e a criação da ARPAnet, em 1969, começou uma nova era.

Nos anos 70 várias instituições já tinham redes de computadores e capacidade tecnológica para processamento de dados pessoais. Era notório o tratamento em massa de dados pessoais feitos quer por instituições privadas quer por instituições públicas.

Sem um regime específico de protecção dos titulares dos dados, aplicou-se por analogia a tutela da reserva da vida privada, nomeadamente o artigo 8º n.º 1 da CEDH, uma vez que se visava proteger as pessoas do uso abusivo de informações intimamente relacionadas com elas.

Todavia, um Estudo do Comité de Ministros do Conselho da Europa concluiu que a CEDH e direito nacional dos Estados não garantia protecção suficiente aos dados pessoais dos indivíduos.

Por isso, o Conselho da Europa, no seu Comité de Ministros aprovou duas resoluções relativas à protecção de dados pessoais: a resolução (73) 22 relativa à protecção da privacidade dos indivíduos face às bases de dados electrónicas no sector privado,

aprovada em 26 de Setembro de 1973[15] e a resolução (74) 29, aprovada em 20 de Setembro de 1974[16].

A primeira centrava-se na protecção da privacidade dos indivíduos face à recolha e tratamento de dados pessoais, pelo sector privado. Para efeitos da protecção só eram consideravam dados pessoais os dados relativos a pessoas físicas, ou seja, empresas ou entidades colectivas não era protegidas por esta resolução.

O anexo da Resolução enunciava um leque de princípios aplicáveis à recolha e tratamento de dados. A recolha dos dados deveria ser feita de forma lícita, pelo que a quantidade de dados pessoais recolhidos deveriam ser proporcionais aos fins a que se destinavam. Após a recolha os dados deveriam ser mantidos exactos e actuais, conservados pelo período de tempo estipulado na lei e sempre adstritos aos fins para que foram recolhidos. No caso de os dados serem utilizados para outros fins, era necessária autorização do titular dos dados. Este tinha direito de aceder às suas informações, saber os fins para que era utilizadas e as transmissões dos dados a terceiros. A fim de garantir a segurança dos dados, o responsável pelo banco de dados devia tomar as medidas de segurança necessárias para evitar perda de informações e intromissão ilícita no banco de dados.

Sempre que os dados a recolher pudessem originar uma discriminação negativa, a sua recolha era proibida, mas no caso de esta já ter ocorrido, a transferência destes dados era vedada.

A segunda Resolução tratava da protecção de dados pessoais relativamente a bancos de dados no sector público. Esta resolução aplica os mesmos princípios da resolução anterior ao sector público, embora com algumas adaptações dados as finalidades dos vários bancos de dados do sector público. Salienta a necessidade de os dados recolhidos serem adequados e apropriados às finalidades a que se destinam e não meramente

[15] Texto integral em https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2.
[16] Texto integral em https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2.

proporcionais, devendo os mesmos serem corrigidos ou apagados caso se mostrem inexactos, desactualizados ou incorrectos.

Dados relativos à intimidade dos indivíduos, que no sector privado não podiam ser recolhidos e tratados, podiam sê-lo pelo sector público, caso a lei ou outra regulação assim o permita.

A limitação temporal da conservação dos dados pessoais também podia sofrer excepções, especificamente quando os dados são conservados para fins estatísticos, históricos ou científico, mas sem afectar a privacidade do indivíduo.

Embora estas resoluções tenham sido o ponto de partida para a legislação sobre a protecção de dados pessoais, elas careciam de força vinculativa, deixando aos Estados – Membros a decisão da sua aplicação e os meios pelos quais a fazem.

O contínuo crescimento do uso de computadores quer em entidades públicas como em empresas privadas e a elaboração de ficheiros com dados pessoais, cuja partilha era facilitada pela internet e pelas telecomunicações, punha em causa a protecção desses dados, uma vez que eles podiam ser transmitidos para outros países, com uma lei de protecção de dados distinta ou até sem legislação aplicável. Além disso os Estados Membros do Conselho da Europa não adoptaram de forma igual os princípios constantes das resoluções, o que dificultava uma protecção dos dados pessoais homogénea além fronteiras.

Em resposta a estas situações, o Conselho da Europa aprovou em 1981 a Convenção 108 relativa ao tratamento de dados pessoais, vinculando os seus signatários, no sentido de harmonizar a legislação sobre protecção de dados pessoais nos países signatários.

3. As novas ameaças à privacidade

Actualmente, a Internet permite o acesso ao correio electrónico, a pesquisa de um indeterminado número de informações, a consulta de variadas bases de dados, partilhar experiências em grupos de discussão e até adquirir produtos e serviços.

O desenvolvimento da tecnologia e da Internet trouxe uma nova realidade à nossa Sociedade. Se antes os dados pessoais eram considerados como propriedade da pessoa e por isso um bem privado dela, protegido pelo direito à privacidade ou reserva da vida privada, a evolução da sociedade para uma sociedade da informática e da tecnologia elegeu os dados pessoais como bem essencial para a manutenção e desenvolvimento da mesma, tornando-os bens semi - públicos. Os dados pessoais são utilizados nos vários sectores da economia, sendo fulcrais, por exemplo, para saber o interesse das pessoas em novos produtos e serviços.

Em certo sentido, cada pessoa corresponde a uma pessoa electrónica. O nosso dia a dia pode ser registado, desde os produtos que compramos no supermercado, em que registamos um cartão de fidelização, até as nossas actividades na internet, que ficam registadas no servidores dos vários agentes presentes na Internet.

Contudo, apesar da sua importância para a economia, os dados pessoais estão relacionados com uma pessoa e o seu tratamento pode implicar violações na sua privacidade.

Se nos anos 70 do século XX a principal preocupação era regular a criação de bases de dados pessoais por empresas e organizações públicas, actualmente a preocupação é regular a reutilização desses dados pelos operadores de serviços, evitando que sejam usados abusivamente.

III. Enquadramento jurídico do tratamento de dados na internet

1. Constituição da República Portuguesa

A CRP consagra no seu artigo 35º o direito à protecção de dados pessoais. Este pode ser qualificado como direito especial de personalidade, uma vez que visa proteger o cidadão dos perigos que o uso da informática pode causar na sua privacidade, mormente no tratamento e uso dos seus dados pessoais. Este direito consagra um leque de direitos fundamentais que permitem que o cidadão seja encarado como pessoa em si e não como objecto de informações, protegendo a dignidade da pessoa como tal. Garante-se o direito à informação sobre os dados pessoais (conhecer, aceder e saber os fins para que são utilizados os dados pessoais), direito de rectificação e actualização dos dados, tal como o direito à eliminação dos mesmos.

A sua consagração na versão original da Constituição foi pioneira, tendo influenciado a legislação de protecção de dados pessoais na Europa.

A consagração deste direito teve influência do direito à autodeterminação informacional. Este direito foi construído inicialmente pela jurisprudência alemã, como uma garantia ao direito geral da personalidade, como demonstra o caso da Lei do Censo de 1950 (BVERFGE 65, 1[17]). A Lei Fundamental da República Federal Alemã não consagrou explicitamente o direito à protecção de dados pessoais, no entanto protege-o com base na dignidade da pessoa humana e do direito geral da personalidade.

A autodeterminação implica conhecimento para agir, o indivíduo só terá liberdade de decisão se tiver conhecimento suficiente para decidir se deve agir ou não. Por isso, a autodeterminação informacional implica que o individuo possa conhecer que dados foram divulgados, quando e a que destinatários, para que possa agir em conformidade para os proteger. No caso de o indivíduo não conseguir determinar que informações

[17] Este caso refere-se à lei de recenseamento de 1950 que previa que os dados recolhidos na realização de um censo, para além de permitirem conhecimento do crescimento da população e da sua distribuição espacial, seriam comparados com registos públicos e transmitidos a repartições públicas, estaduais e municipais para fins de execução administrativa.

foram divulgadas e a quem, não vai poder exercer o controlo em segurança, afectando a sua liberdade de decisão. Por isso, têm que existir regras quanto ao tratamento de dados que permitam que o titular dos dados tenha conhecimento desses dados e possa controlar o seu uso.

Podemos apresentar este direito à autodeterminação informacional como direito de liberdade com uma dupla dimensão: a de direito de protecção, de índole negativo, que visa impedir as ingerências do Estado e de privados, podendo o indivíduo recusar a divulgação de informações pessoais ou opor-se ao tratamento das mesmas; a de liberdade, em sentido positivo, prevendo o poder do indivíduo determinar o uso das suas informações pessoais.

GOMES CANOTILHO[18], defende que os vários direitos consagrados no artigo 35º incorporam este direito à autodeterminação informacional, permitindo que o cidadão tenha controlo sobre os seus dados.

2. Directiva 95/46/CE

A crescente utilização de dados pessoais e a necessidade de harmonizar o mercado único entre os Estados – Membros, impeliu a União Europeia a regular a matéria da protecção de dados pessoais.

Tendo como modelo a Convenção 108 do Conselho da Europa, o Parlamento Europeu e o Conselho Europeu apresentaram uma proposta de directiva a 27 de Julho de 1990, que após processo de discussão, foi adoptada a 24 de Janeiro de 1995.

A directiva estendeu o seu âmbito de aplicação, aplicando-se também ao tratamento de dados através de ficheiros manuais, tal como enunciado no artigo 3º da DP: o *tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como o tratamento por meios não automatizados de dados pessoais contidos num*

[18] GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, Vol. I, 4ª Edição, Coimbra, Coimbra Editora, 2007, p. 551.

ficheiro ou a ele destinados. Ou seja, também se aplica aos tratamentos de dados feitos por meios informáticos, uma vez que implicam meios automatizados.

Para proteger os dados pessoais face a um tratamento e uso abusivo, a directiva estabeleceu um conjunto de princípios reguladores do tratamento de dados pessoais automatizado ou não automatizados, aplicáveis ao responsável pelo tratamento.

O princípio do consentimento é central no regime de protecção de dados pessoais, uma vez que o tratamento dos mesmos depende, regra geral, do consentimento inequívoco do titular dos dados, não sendo assim quando o tratamento se torna necessário à *execução de contrato, de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido*; *ou para cumprimento de obrigação legal do responsável pelo tratamento; para protecção de interesses vitais do titular dos dados; execução de uma missão de interesse público ou no exercício de autoridade pública em que o responsável pelo tratamento esteja investido; ou prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados foram comunicados* (artigo n.º 7º DP).

Os princípios da lealdade e da licitude implicam que o titular dos dados tenha conhecimento do tratamento dos dados e que este obedeça a todas as normas nacionais, internacionais e europeias aplicáveis. Logo aquando da recolha dos dados, ela tem que ser feita junto da pessoa em causa, devendo o responsável pelo tratamento identificar - se e explicar o tratamento de dados a efectuar, especificamente as finalidades do mesmo, os destinatários a quem os dados vão ser comunicados e o carácter facultativo ou não das respostas na recolha dos dados pessoais. Deve ainda informar os direitos do titular dos dados, nomeadamente, o direito de acesso e o direito de rectificação.

O princípio da qualidade dos dados consiste em os mesmos serem adequados, pertinentes e não excessivos em razão das finalidades do tratamento de dados. Têm que ser exactos, pelo que devem ser actualizados ou corrigidos, sempre que se mostrem inexactos ou incorrectos. Além disso, os dados deverão ser conservados de forma a identificar o titular dos dados apenas pelo período estritamente necessário.

O princípio da finalidade determina que os dados recolhidos sejam tratados para as finalidades determinadas no momento da recolha dos dados, devendo estas ser explícitas e legítimas.

O princípio da não interconexão que obriga a entidade responsável pelo tratamento a não comunicar os dados pessoais recolhidos a entidades que não realizem as mesmas finalidades. A interconexão de dados está sujeita a autorização, no caso português a CNPD, a autoridade portuguesa de supervisão relativamente à matéria da protecção de dados pessoais, excepto quando a interconexão seja prevista em disposição legal.

O não cumprimento destes princípios pode implicar a aplicação de sanções, tal como previsto no artigo 24º da DP.

A LPDP prevê no seu artigo 38º a aplicação de uma coima mínima de 498, 80€ e máxima de 4.988€ às entidades que não cumprirem obrigações relativas ao tratamento de dados pessoais, nomeadamente os princípios anteriormente expostos.

Para além dos princípios acima enunciados, a directiva atribui um leque de direitos ao titular dos dados: direito de informação, direito de acesso, direito de rectificação e direito de oposição.

O direito de informação é o direito de o titular dos dados conhecer que dados vão ser recolhidos e a sua pertinência, os destinatários a quem os dados vão ser comunicados, as finalidades para que estão a ser recolhidos, os direitos que lhe assiste durante o tratamento dos dados e a identificação do responsável pelo tratamento ou o seu representante.

O direito de acesso é o direito do titular de dados obter do responsável pelo tratamento informações sobre os seus dados pessoais. De acordo com este direito o titular de dados pode livremente, sem demoras e sem encargos excessivos saber se os seus dados pessoais estão a ser alvo de tratamento, e se o estiverem a ser, para que fins estão a ser tratados, que categorias de dados são objecto de tratamento, a que destinatários vão os mesmos ser comunicados e a origem dos dados pessoais. O responsável pelo tratamento deve comunicar estas informações de um modo acessível. Quando estiver em causa

tratamento automático de dados, o titular dos dados tem direito a saber qual a lógica subjacente a esse tratamento.

O direito de rectificar, apagar ou bloquear é direito do titular rectificar, apagar ou bloquear os seus dados pessoais quando o tratamento dos mesmos não cumprir as regras presentes na directiva e especificamente quando os dados estejam inexactos e incompletos. Sendo exercido este direito, o responsável pelo tratamento deve notificar terceiros a quem os dados tenham sido reportados, a sua rectificação, apagamento ou bloqueio, excepto se for impossível ou implicar um esforço desproporcionado.

O direito de oposição é o direito da pessoa em causa se opor ao tratamento dos seus dados pessoais quando este é realizado devido a interesse público ou exercício da autoridade pública pelo responsável pelo tratamento ou terceiro, a quem os dados foram reportados. A pessoa em causa pode-se opor apresentando razões preponderantes e legítimas relacionadas com a sua situação particular. É permitido ainda à pessoa em causa se opor *a priori* ao tratamento dos seus dados para efeitos de mala directa[19].

3. Directiva relativa à privacidade e às comunicações electrónicas (directiva 2002/58/CE)

Esta directiva regula o tratamento de dados pessoais e a protecção da privacidade no âmbito das prestações de serviços de comunicações electrónicas acessíveis ao público em redes de comunicações públicas.

É de notar que a Internet é um serviço de comunicação electrónica, uma vez que consiste no envio de sinais através de redes de comunicações públicas[20], pelo que os tratamentos de dados pessoais feitos através da Internet estão sujeitos à aplicação desta directiva.

[19] Mala directa ou marketing directo consistem numa prática de propaganda de serviços dirigida a um grande número de consumidores, mas endereçada individualmente. Permite uma relação mais personalizada com o cliente e facilita a fidelização do mesmo. Ver em:http://pt.wikipedia.org/wiki/Marketing_direto.

[20] Artigo 2º al. b) da Directiva 2002/21/CE.

Todavia se os dados forem recolhidos e tratados no âmbito de uma rede privada (por exemplo, rede privada de uma entidade pública), por ser uma rede de comunicações não acessível ao público, não lhe é aplicável a directiva 2002/58/CE. O tratamento de dados é, neste caso, regulado pela Directiva 95/46/CE.

Além disso, só se aplica aos dados tratados no âmbito de prestações de serviços de comunicações electrónicas. A directiva 2002/21/CE define estes serviços no seu artigo 2º al.c) como "o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações electrónicas (…)". É este o caso do ISP, IAP e operadores de telecomunicações.

Para garantir privacidade aos utilizadores de Internet esta directiva regula o período de conservação dos dados recolhidos no âmbito das comunicações electrónicas: dados de tráfego e de localização.

Os dados de tráfego só podem ser conservados pelo período necessário para efectivar a transmissão da comunicação, pelo que depois deverão ser eliminados ou tornados anónimos. Todavia, do conjunto de dados que incorporam os dados de tráfego podem ser armazenados e tratados os necessários para efeitos de facturação, e até quando a factura puder ser legalmente contestada ou o pagamento reclamado.

Os dados de localização, regra geral, só podem ser tratados se forem anónimos, no entanto o utilizador das redes de comunicação pode consentir na recolha e tratamento desses dados, devendo ser mantidos na medida no necessário e pelo período estritamente necessário para a prestação de serviços de valor acrescentado[21].

É de notar que a directiva 2006/24/CE, de 15 de Março de 2006, veio alargar o prazo de conservação de dados de tráfego e de localização. Estabeleceu a obrigação de conservar determinados dados, indicados no artigo 5º dessa directiva, pelo prazo não inferior a 6 meses e não superior a 2 anos.

[21] São serviços de valor acrescentado aqueles que requeiram o tratamento de dados de localização que não sejam dados de tráfego associados à facturação ao envio da comunicação.

A Lei n.º32/2008, de 17 de Julho, que transpôs esta directiva para a ordem jurídica Portuguesa, delimita no seu artigo 6º que os dados devem ser conservados pelo período de 1 ano a contar da conclusão da transmissão.

Relativamente ao uso de *cookies* esta directiva determinou que as entidades que queiram utilizá-los têm que ter o consentimento prévio dos utilizadores de Internet e informar de forma clara e completa os utilizadores sobre o uso de *cookies*.

Pode-se ler no artigo 5º n.º3 da directiva 2002/58/CE que "Os Estados Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento".

No âmbito da instalação de *cookies* e da necessidade de informar os utilizadores e pedir o seu consentimento pode-se consultar o *Procedimiento* nº PS/00321/2012[22] da Autoridade Espanhola de Protecção de dados (AEPD). Neste caso a AEPD instaurou um processo contra duas entidades com o fundamento de as suas páginas *Web* não cumprirem as disposições relativas aos cookies. Neste mesmo documento a AEPD refere um conjunto de informações que devem estar indicadas nas páginas *Web* que utilizam *cookies*, nomeadamente:

- Aviso do uso de *cookies* ao aceder à página *Web* ou utilizar o serviço;
- Referir as finalidades das *cookies* instaladas e se são *cookies* do próprio ou de terceiros.
- O tipo de *cookie*, a sua definição e forma de desactivá-la.

No entanto a directiva também prevê excepções relativamente ao consentimento para instalação de *cookies*, sempre que estes sejam necessários para transmitir uma comunicação através da Internet ou fundamentais para o fornecer um serviço solicitado pelo utilizador da Internet (artigo 5º n.º 3 *in fine* da directiva 2002/58/CE).

[22] Disponível em http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php.

É o caso dos *cookies* de autenticação, presentes nas páginas *Web* de bancos. O cliente do banco apenas tem que se identificar para iniciar a sessão, não tendo que repetir quando acede aos movimentos de conta ou aos mútuos associados à sua conta bancária.

4. Coordenação da aplicação da directiva 95/46/CE e da directiva 2002/58/CE

Os dados recolhidos e tratados através Internet, desde que possam identificar a pessoa em causa, são qualificados como dados pessoais e desse modo sujeitos à aplicação da directiva geral sobre tratamento de dados pessoais. No entanto, como referido no número anterior, sendo dados recolhidos e tratados através da Internet no âmbito da prestação de serviços de comunicações electrónicas acessíveis ao publico em redes de comunicações públicas estão sujeitos à aplicação da directiva sobre protecção da privacidade nas comunicações electrónicas.

Deste modo, os fornecedores de acesso à Internet, os fornecedores de serviços de internet e os operadores de telecomunicações estão sujeitos à aplicação de ambas as directivas. Os titulares de páginas de Internet e qualquer entidade que utilize a internet para recolher e tratar dados estão sujeitos à aplicação da directiva geral sobre tratamento de dados.

Todos os agentes devem requerer o consentimento dos utilizadores de Internet para recolher os seus dados e tratá-los, informando-os das finalidades do tratamento, dos direitos que lhes são atribuídos e da sua própria identificação para que os possam exercer. Nas situações em que o próprio utilizador disponibiliza os dados, este deve referir clara e expressamente o seu consentimento.

Há que ressalvar neste caso os IAP, ISP e operadores de telecomunicações. Estas entidades recolhem dados pessoais no âmbito da prestação de serviços contratados com o utilizador, pelo que não necessitam requerer o consentimento dos titulares dos dados.

Todos os dados recolhidos devem ser necessários e adequados às finalidades do tratamento, devendo ser eliminados ou tornados anónimos quando não forem

necessários ao tratamento, excepto quando por lei se imponha a sua conservação por período superior.

5. Proposta de Regulamento Geral sobre protecção de dados[23].

A apresentação desta proposta pelo Parlamento Europeu e a Comissão Europeia tem dois objectivos: proteger os dados pessoais, que com a crescente evolução tecnológica estão sujeitos a novos riscos e criar a confiança dos consumidores nos serviços em linha.

Se por um lado, a evolução tecnológica permitiu às entidades públicas e privadas recolherem e tratarem cada vez mais dados, no exercício das suas actividades, os próprios titulares dos dados os divulgam de forma pública e global, nomeadamente nas redes sociais. O uso e tratamento de dados pessoais são generalizados. Foi por isso necessário repensar o regime de protecção de dados pessoais.

Por outro lado, o desenvolvimento económico passa cada vez mais pela internet: pela disponibilização de serviços e produtos na rede, pela facilidade de promoção, uma vez que um número indeterminado de pessoas acede à internet todos os dias em todo o mundo.

A proposta vem concretizar a directiva 95/46/CE, apresentando mais detalhadamente os princípios sobre tratamento de dados e os direitos atribuídos aos titulares dos dados. Apresenta também inovações face a esta directiva.

Introduz o princípio da transparência, determinando no seu artigo 11º que devem ser aplicadas "regras transparentes e de fácil acesso relativamente ao tratamento de dados pessoais e ao exercício dos direitos pelos titulares de dados". Logo quaisquer comunicações e informações sobre o tratamento dos dados devem ser dadas de "forma inteligível, numa linguagem clara e simples, adaptada à pessoa em causa".

[23] COM (2012) 11 final - Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Bruxelas, 25/01/2012.

Reforça, no seu artigo 5º al. c), a necessidade de a recolha dos dados ser proporcional e necessária, pois deve-se limitar ao mínimo necessário face às finalidades do tratamento. Além disso os dados pessoais só podem ser recolhidos se as finalidades do tratamento não possam ser alcançadas através de informações não qualificadas como dados pessoais.

Consagra ainda o princípio da responsabilidade do responsável pelo tratamento, na al. f) do artigo 5º. O responsável terá que garantir e demonstrar a conformidade das operações de tratamento com o regulamento.

É de salientar a introdução da avaliação de impacto sobre a protecção de dados e a designação de um delegado para a protecção de dados.

A avaliação do impacto sobre a protecção de dados é realizada obrigatoriamente sempre que a natureza dos dados, o âmbito e as finalidades do tratamento representem um risco para os direitos e liberdades dos titulares. Essa avaliação deve ser feita, por exemplo, quando há um tratamento automatizado de dados genéticos ou biométricos.

Sempre que a avaliação conclua que existe um elevado nível de riscos específicos para os direitos e liberdades dos titulares antes de iniciar o tratamento dos dados o responsável pelos dados ou o subcontratante deve consultar a autoridade de controlo.

O delegado para a protecção de dados tem como atribuições auxiliar o responsável pelo tratamento ou o subcontratante no cumprimento de todas as disposições do regulamento, sendo o ponto de contacto com a autoridade de controlo e com os titulares de dados, que lhe podem endereçar os seus pedidos de informação ou de exercício de direitos conferidos pelo regulamento.

A designação do delegado para a protecção de dados depende de características do responsável pelo tratamento. Só autoridades ou organismos públicos; empresas com 250 assalariados ou mais; ou responsáveis pelo tratamento, cujas actividades principais tenham especificidades que impliquem um controlo "regular e sistemático dos titulares dos dados", estão sujeitas a essa obrigação. Fora dessas situações, a designação é facultativa.

A PR reforça a segurança dos dados pessoais, introduzindo um conjunto de medidas a tomar pelo responsável pelo tratamento quando se verifique uma violação de dados pessoais. Primeiro terá que notificar a autoridade de controlo no prazo máximo de 24 horas (artigo 31º n.º1 da PR) e posteriormente comunicar ao titular dos dados a violação de dados pessoais, quando se verifique que essa violação afecta negativamente a protecção dos seus dados pessoais ou a sua privacidade (artigo 32º n.º1 da PR).

A PR prevê ainda, no seu artigo 64º, a criação do Comité Europeu para a protecção de dados, cuja função é assegurar a aplicação coerente do regulamento, através de elaboração de recomendações, directrizes e boas práticas para as autoridades de controlo, e a fiscalização da sua aplicação prática.

II. O direito a ser esquecido e ao apagamento

O direito a ser esquecido (*right to be forgotten*) é o direito da pessoa requerer a eliminação dos seus dados pessoais, das referências e ligações aos mesmos, para que terceiros não os conheçam. Tem como base a ideia de autonomia do titular dos dados, como detentor dos seus dados pessoais. Este direito está previsto no Regulamento Geral de Protecção de Dados Pessoais e tem sido alvo de muita discussão, dadas as possíveis limitações à liberdade de expressão, à liberdade de informação, à informação histórica e estatística.

1. Ratio legis

O incremento do acesso à internet, a partir dos anos 90 do séc. XX, e o desenvolvimento tecnológico criaram novos riscos para a protecção de dados pessoais. Qualquer fotografia, comentário ou informação que se divulgue em blogs, redes sociais ou outras páginas - fonte, fica permanentemente na Internet. Além disso a facilidade com que os utilizadores de internet acedem à informação através dos motores de busca e a capacidade tecnológica actual que detêm para a copiarem e guardar, possibilita a divulgação das informações e a conservação da mesma por um período indeterminado, sendo difícil ou até impossível ao sujeito a que se referem as informações (titular dos dados) controlar o uso e tratamento das mesmas.

As redes sociais são exemplo paradigmático desta realidade. Qualquer fotografia descarregada na rede social, comentário realizado ou aplicação utilizada é registada permanentemente no servidor da rede social e pode ser visionada por qualquer utilizador da rede, caso o titular dos dados não defina padrões de privacidade na sua conta na rede social. Esta situação foi comprovada por um estudante austríaco que, ao abrigo do direito de acesso, requereu a comunicação dos dados que a rede social a que era aderente detinha sobre ele. Verificou que a rede social mantinha toda a sua actividade na rede social registada, inclusive as informações que tinha eliminado.

Para além das situações em que o próprio sujeito divulga informações sobre si, há que atender ainda às situações em que a recolha de dados é feita passivamente, sem que o sujeito tenha conhecimento, sendo impedido de efectuar o controlo sobre o uso dos seus dados. É exemplo disso os *cookies*, analisados anteriormente neste trabalho.

Mesmo quando o sujeito toma medidas para proteger os seus dados na internet, o desenvolvimento de softwares de correspondência de dados, para criação de perfis, e identificação de dados anónimos dificulta a protecção pelo próprio titular dos dados.

Por fim, economicamente os custos para manter os dados pessoais são mais baixos do que eliminá-los ou torná-los anónimos, por isso a tendência das entidades responsáveis pelo tratamento de dados tem sido mantê-los[24].

Perante esta realidade, houve a necessidade de reforçar os direitos das pessoas principalmente no contexto da internet. A Comissão Europeia e o Parlamento Europeu propuseram a criação de um novo direito para o titular de dados: o direito a ser esquecido e ao apagamento que é definindo como o "*direito de obter do responsável pelo tratamento o apagamento de dados pessoais que lhe digam respeito e a cessação da comunicação ulterior desses dados (...)*".

2. Regime proposto

O regime jurídico proposto atribui ao titular dos dados o direito à eliminação dos seus dados pelo responsável do tratamento e o término do seu processamento, quando se verificar uma das situações seguintes:

- quando os dados já não sejam necessários para a finalidade enunciada aquando da sua recolha; quando o consentimento de recolha e tratamento foi retirado;

- quando o período de conservação dos dados terminou e não exista fundamento jurídico para continuar o tratamento;

[24] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS PESSOAIS, Opinião de 14 de Janeiro de 2011, parágrafo 84. Disponível em: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf

- quando o titular dos dados se opõe ao tratamento; e

- quando o tratamento dos dados desrespeita alguma das disposições do regulamento.

Apesar de aparentemente o leque de fundamentos para eliminação dos dados ser fechado, o facto deste direito poder ser exercido quando o tratamento dos dados desrespeita alguma das disposições do regulamento, permite a aplicação deste direito a outras situações, nomeadamente, quando o responsável pelo tratamento não cumpre a obrigação de informar o titular dos dados, regulada no artigo 14º da PReg, ou quando os dados foram tratados sem o consentimento do titular, sendo o tratamento ilícito, de acordo com o artigo 6º n.º1 al. a) da PReg. Todas as situações em que se pode exercer o direito ao esquecimento são objectivas, ou seja, tem que se verificar uma situação concreta que justifique esse apagamento. A simples preferência do titular dos dados de que os dados sejam eliminados não parece fundamentar o exercício deste direito.

Para exercer este direito o titular dos dados deve requerer ao responsável pelo tratamento a eliminação dos seus dados e posterior cessão do tratamento. O responsável pelo tratamento deverá responder se defere ou não o pedido, no prazo de um mês a contar da recepção do mesmo (artigo 12º n.º 2 da PReg). No caso de indeferir o pedido, o responsável pelo tratamento deve fundamentar a conclusão.

Deferindo o pedido o apagamento deve ser feito sem demora. Contudo atendendo a que o direito "a ser esquecido" não é um direito absoluto, o legislador previu, no n.º 3 do artigo 17º da PReg, situações em que apesar do titular dos dados requerer o apagamento dos seus dados, a conservação dos mesmos é necessária para a protecção de outros direitos e interesses, como por exemplo, o direito de liberdade de expressão e a conservação para fins de investigação histórica, estatística ou científica.

Quando o responsável pelo tratamento dos dados os tenha tornado públicos deve tomar todas as medidas razoáveis para comunicar a terceiros o pedido de apagamento dos dados, tal como quaisquer ligações, cópias e reproduções dos mesmos. O Grupo de trabalho do artigo 29º ressalva que o responsável pelo tratamento pode não comunicar com todas as pessoas ou entidades que têm cópias dos dados objecto de eliminação pois pode não ter conhecimento da localização de todas as cópias. Salienta ainda que, a PReg

não obriga terceiros a cumprirem com o pedido do titular dos dados, se esses terceiros não poderem ser qualificados como responsáveis pelo tratamento, por isso é necessário clarificar a posição destes quanto ao cumprimento do pedido do titular dos dados e as consequências para o não cumprimento[25].

Além disso a PReg não prevê as situações em que o responsável pelo tratamento já não existe e não pode ser contactado. O Grupo de trabalho do artigo 29º propõe que o direito a ser esquecido seja aplicado também a terceiros que processam dados, de forma que o titular dos dados possa requerer a eliminação dos dados directamente a esses terceiros, quando não o possa requerer ao responsável pelo tratamento ou quando esse processamento não foi autorizado pelo responsável[26].

Com vista a contornar a ambiguidade da aplicação do bloqueio de dados, regulado na directiva 95/46/CE, a PReg prevê um conjunto de situações em que o responsável pelo tratamento deve restringir o tratamento dos dados em vez de os eliminar. Assim quando os dados sejam considerados inexactos pelo titular dos dados, mas a sua exactidão possa ser restabelecida pelo responsável pelo tratamento; os dados tenham que ser mantidos para efeitos de prova; o titular se opuser à eliminação dos dados, apesar de o tratamento ser ilícito; ou quando o titular exerceu o direito de portabilidade dos dados (artigo 18º da P. Reg), o responsável pelo tratamento deverá restringir o tratamento desses dados em vez que os eliminar (artigo 17º n.º4 da P. Reg).

O regime proposto vem clarificar e reforçar os princípios da finalidade, da qualidade e do consentimento.

Apesar de no artigo 12.º, alínea b) da directiva se possibilitar o apagamento ou bloqueio dos dados quando haja violação de alguma disposição da directiva, a consagração explícita das situações em que poderá ser exercido poderá impulsionar o efectivo cumprimento daqueles princípios, mesmo que por exigência dos titulares dos direitos.

---

[25] GRUPO DE TRABALHO DO ARTIGO 29º, "Opinião 01/2012 sobre as propostas de reforma do regime de protecção de dados pessoais", adoptada em 23 de Março de 2012, página 13. Disponível em http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/index_en.htm.

[26] Nos termos do art. 17º n.º3 da PReg quando o responsável pelo tratamento autorizar a publicação de dados por terceiros torna-se também responsável por essa publicação.

Além disso, a previsão da possibilidade de retirar o consentimento vem clarificar os direitos atribuídos aos titulares de dados, pois na directiva 95/46/CE não estava prevista a possibilidade de retirar o consentimento, apesar de já se entender que tendo o indivíduo a possibilidade de dar consentimento, também teria a possibilidade de retirar o consentimento.

3. Direito a ser esquecido: Domínio Penal

Historicamente, o direito a ser esquecido foi consagrado no domínio penal através da jurisprudência. Este direito impedia a publicação de notícias ou divulgação de programas televisivos relacionados com condenações penais, especificamente quando se revelasse a identidade da pessoa condenada, sempre que essa publicação não seja relevante e necessária para a Sociedade Civil. Garantia-se desta forma que a reintegração da pessoa na Sociedade e uma oportunidade de recomeçar a sua vida. Contudo, este direito não era absoluto e por isso sempre que se justificasse, a identidade da pessoa e factos relacionados à sua condenação podiam ser publicados, dando assim prevalência ao direito à informação.

O Caso Lebach[27] refere-se à emissão de documentário sobre um homicídio de quatro soldados ocorrido em Lebach, na Alemanha, em data próxima da libertação de um dos autores do crime. Nesse documentário o crime seria reconstituído, referindo os nomes, fotografias e informações específicas sobre cada autor do crime. O Tribunal Constitucional Alemão considerou que estavam em colisão a liberdade de expressão e o direito de personalidade do indivíduo. Não podendo hierarquizar estes dois direitos e não podendo compatibilizá-los, analisou as particularidades do caso e concluiu que o documentário não podia ser emitido caso referisse informações sobre o autor, uma vez que divulgando informações sobre o autor associadas a este crime, tão perto da data em que terminava a pena de prisão, afectaria negativamente a sua possibilidade de reintegração.

[27] BVerfGE 35.

O Caso R. AG[28] refere-se à divulgação num jornal da condenação por crimes económicos de um administrador de uma empresa. O lesado instaurou um processo contra o jornal e o autor do artigo por violação do direito de privacidade. O Tribunal Federal Suíço considerou que a divulgação do passado criminal do autor era desnecessária, uma vez que não existia interesse público e punha em causa a reabilitação do autor. O Tribunal concluiu que existia uma violação do direito a ser esquecido.

4. Direito a ser esquecido na directiva 95/46/CE

Considerado um pilar da reforma da regulação de protecção de dados pessoais, a consagração do direito a ser esquecido e ao apagamento é considerada uma inovação no panorama da protecção de dados pessoais.

No entanto, há quem considere que a directiva 95/46/CE já consagrava o direito a ser esquecido de modo implícito, por via da conjugação do princípio da finalidade e da qualidade dos dados[29].

A conservação dos dados pessoais deve ser limitada. Quando os dados já não sejam necessários e adequados às finalidades do tratamento dos dados, eles devem ser eliminados ou tornados anónimos. Se o responsável pelo tratamento não o fizer, o titular dos dados tem o direito de obter do responsável, a eliminação ou o bloqueio dos dados, de acordo com o artigo 12º al. b) da directiva[30].

Em decorrência deste direito implícito, o direito à oposição, regulado no artigo 14º da directiva, permite ao titular dos dados se opor ao tratamento dos dados no caso do tratamento dos mesmos ser necessário para o responsável pelo tratamento ou terceiros devido a interesses legítimos dos mesmos. Para exercer este direito o titular dos dados

[28] BGE 122 III 449
[29] CASTRO, CATARINA SARMENTO E, "Direito da Informática, privacidade e dados pessoais", Coimbra, Almedina, 2005, p. 240.
[30] CASTELLANO, PERE SIMÓN, "The right to be forgotten under European Law: a Constitucional debate", Lex Electronica, vol. I. 16.1 (Hiver /Winter 2012), página 6; DE TERWAGNE, CÉCILE, "Privacidad en Internet y el derecho a ser olvidado /derecho al olvido", 2012, página 58.

tem que demonstrar que razões "preponderantes e legítimas relacionadas com a sua situação particular[31]" impedem a continuação do tratamento dos dados.

As autoridades de Protecção de dados pessoais francesa, italiana e espanhola, têm reconhecido este direito a ser esquecido no âmbito da directiva 95/46/CE. Exemplo disso é o processo intentado pela Google Spain e Google Inc contra a APED (Autoridade Espanhola de Protecção de dados).

O caso em questão é o de um cidadão espanhol que foi sujeito a uma venda de um imóvel em hasta pública devido a dívidas à Segurança Social. A venda foi divulgada num jornal espanhol, acompanhada dos nomes e apelidos dos proprietários sujeitos à medida. Dez anos decorridos, o cidadão requereu ao editor do jornal e à Google o apagamento dos dados e da hiperligação para as páginas do jornal, respectivamente. Perante a oposição de ambos, o cidadão apresentou uma reclamação junto da Autoridade Espanhola para a Protecção de Dados (APED), para que o seu nome e apelidos fossem apagados da página do jornal ou deixassem de ser exibidos no motor de pesquisa da Google. A reclamação foi deferida quanto à Google e indeferida quanto ao editor do jornal, uma vez que a publicação da noticio pelo jornal era lícita, tendo sido feita por Ordem do Ministério do Trabalho e dos Assuntos Sociais. A Google Spain e a Google Inc intentaram um processo junto da *Audiencia Nacional* para que a decisão da APED fosse declarada nula.

O Tribunal em questão suspendeu o processo e requereu a decisão do Tribunal de Justiça sobre um conjunto de questões prejudiciais, nomeadamente a de saber se o direito de apagamento e bloqueio de dados, regulados no artigo 12º, alínea b) e o direito de oposição regulado no artigo 14º, alínea a) da Directiva 95/46/CE, permitem a uma pessoa impedir que os motores de pesquisa indexem informação referente a si, porque a publicação dessa informação a prejudica ou quer que a mesma seja esquecida, apesar de a informação ter sido publicada licitamente por terceiros.

O advogado – geral, nas suas conclusões considerou que " a directiva não prevê um direito genérico «de ser esquecido», no sentido de a pessoa em causa ter o direito de

[31] Art. 14º al. a) da directiva 95/46/CE.

limitar ou de pôr termo à difusão de dados pessoais que considera prejudiciais ou contrários aos seus interesses"[32]. Considerou que tem de existir uma justificação legítima e preponderante para o apagamento ou bloqueio dos dados e para a oposição ao tratamento e não apenas uma "preferência subjectiva". Concluiu ainda que o direito a ser esquecido é uma inovação da proposta de regulamento e não a consagração de um direito já estabelecido[33].

O Tribunal de Justiça da União Europeia considerou que o titular dos dados pode requerer a supressão dos seus dados, de acordo com o artigo 12º al.b) da directiva 95/46/CE, se o tratamento dos dados for incompatível com a directiva, sendo que essa incompatibilidade "pode resultar não só do facto de esses dados serem inexatos mas, em especial, também do facto de serem inadequados, não pertinentes ou excessivos atendendo às finalidades do tratamento, de não estarem atualizados ou de terem sido conservados durante um período de tempo superior ao necessário, a menos que a sua conservação se imponha para finalidades históricas, estatísticas ou científicas."[34]

No caso em apreço, o tribunal considerou que a divulgação de dados pessoais não era pertinente e por isso era inadequada e excessiva, uma vez que já tinham decorrido 16 anos desde o processo de arresto, que entretanto tinha sido resolvido. Logo, o tratamento desses dados pessoais eram incompatíveis com a directiva 95/46/CE e por isso o titular dos dados podia requerer a supressão da informação e das ligações referidas nas listas de resultados apresentadas pela Google.

O Tribunal considerou ainda que o pedido de supressão de dados pelo titular dos dados não tem que necessariamente ser fundamentado pelo prejuízo causado ao titular pela publicação desses dados pessoais. O titular dos dados tem direito a que os seus dados sejam eliminados, retirados, dessa forma, à disponibilidade dos utilizadores da *internet*, com o fundamento nos seus direitos fundamentais: direito ao respeito pela vida privada (artigo 7º da CFUE) e direito à protecção de dados pessoais (artigo 8º da CFUE), porque "esses direitos prevalecem, em princípio, não só sobre o interesse económico do

[32] Processo C -131/12, Conclusões do Advogado – Geral, 25 de Junho de 2013, página 20, parágrafo 108.
[33] Ibidem, página 21.
[34] Processo C-131/12, parágrafo 92.

operador do motor de busca mas também sobre o interesse desse público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa.[35]"

Concluindo, o Tribunal considerou que o titular dos dados tem, em princípio, direito a que os seus dados sejam eliminados das listas de motores de pesquisa, porque tem direito ao respeito pela sua vida privada e pela protecção de dados pessoais. Só assim não se verifica se, em casos excepcionais, o direito de acesso à informação pelo público prevalece sobre os direitos fundamentais do titular dos dados.

A APED tem -se manifestado activa relativamente ao direito ao apagamento, defendendo que indivíduos que não são figuras públicas, mas que no passado foram referidos em notícias, por exemplo, crimes, investigações ou arguidos, devem ter direito a eliminar as notícias que os referenciam. O facto de terem sido associados a este tipo de notícias pode prejudicar a sua reputação, uma vez que essa informação está acessível e pode estar incorrecta, desactualizada ou inexacta, por a situação ter sido esclarecida posteriormente. Defende que nestes casos, o direito à protecção de dados pessoais deve prevalecer face ao direito à informação.

Também a Autoridade de Protecção de Dados francesa - *Commission nationale de l'informatique et des libertés* (CNIL) tem agido relativamente ao direito a ser esquecido, tendo reconhecido a existência deste direito em 1999, no seu vigésimo relatório de actividade. Tem reconhecido a importância deste direito para a protecção das pessoas na internet e na possibilidade destas mudarem de opinião[36]. Além disso, foi apresentada em 2009 em França uma proposta de lei que explicitamente reconhece o direito a ser esquecido. Na exposição de motivos a regulação do direito a ser esquecido surge explicado da seguinte forma:

« Au total, il convient de noter que plusieurs mesures de la présente proposition de loi permettent de donner une plus grande effectivité au **droit à l'oubli numérique,** *(…)* **:l'information spécifique, claire et accessible** *donnée aux personnes, avant tout traitement, mais également de manière permanente, sur le site Internet du responsable*

[35] Ibidem, parágrafo 97.
[36] CNIL, 30e Rapport d' activité 2009, p. 29. Disponível em http://www.cnil.fr/documentation/rapports-dactivite/.

du traitement, de la durée de conservation des données ; la possibilité de demander à la CNIL, pour les traitements déclarés auprès d'elle, la **durée de conservation des données ; l'exercice plus facile du droit d'opposition**, *renommé, pour plus de clarté, droit à la suppression des données, non seulement parce que la proposition de loi précise que ce droit est gratuit, mais également parce que ce droit pourrait désormais être exercé, après identification, par voie électronique, alors que les responsables de traitement prévoient aujourd'hui généralement la seule transmission par courrier postal, de nature à décourager les personnes concernées ;* »[37]

Além disso, visando reforçar a aplicação prática da lei de protecção de dados francesa[38], Nathalie Kosciusko – Morizet, Secretária de Estado responsável pelo desenvolvimento da Economia Digital assinou juntamente com várias empresas da economia digital duas cartas de boas práticas para reforçar a aplicação dos princípios aplicáveis ao tratamento de dados pessoais.

Charte du droit a l'oubli dans les sites collaboratifs et les moteurs de recherche[39], que pode ser traduzido como Carta do direito a ser esquecido em sites colaborativos e motores de pesquisa, foi assinada pela Microsoft França, Skyrock.com, entre outros, 13 de Outubro de 2010. Define um conjunto de orientações a aplicar ao tratamento de dados publicados intencionalmente pelos utilizadores da *internet* que no seu conjunto permitem a aplicação do direito a ser esquecido a esses dados. Esta carta procura garantir o respeito pela vida privada dos utilizadores de *internet* e reforçar o seu controlo sobre os dados publicados.

Esta carta foi assina a 10 de Fevereiro de 2009, no Dia da Internet Segura, pela Comissão Europeia, representada por Viviane Reding e outros agentes presentes na Internet, incluindo Facebook, Youtube e Dailymotion.

---

[37] Proposition de loi *visant à mieux* garantir *le droit à la* vie privée *à l'heure du* numérique, submetida por Yves Détraigne e Anne – Marie Escoffier. Disponível em http://www.senat.fr/leg/ppl09-093.html.

[38] Lei n.º 78-17, de 6 de Janeiro de 1978. Disponível em: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&fastPos=1&fastReqId=1356100880&categorieLien=cid&oldAction=rechTexte

[39] Texto integral em: http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf

A segunda carta foi assinada a 30 de Setembro de 2010 e tem como título *Charte sur la publicite ciblee et la protection des internautes*[40], que pode ser traduzido como Carta sobre publicidade alvo e a protecção dos internautas. A publicidade alvo inclui a publicidade comportamental, que consiste na publicidade apresentada segundo um estudo prévio das escolhas e preferências do utilizador; publicidade contextual, que se refere à publicidade apresentada ao utilizador com base na escolha feita por ele, por exemplo, o utilizador pesquisa sobre livros escolares, é-lhe apresentada publicidade sobre livrarias *on-line*; publicidade personalidade, que é a personalidade directamente dirigida ao utilizador, com base em características do utilizador conhecidas ou por ele indicadas, quando por exemplo, aderiu a um serviço *on-line*.

O estudo do perfil do utilizador, agregando informações sobre ele, pode limitar o seu direito à privacidade, pelo que esta carta visa reforçar o consentimento do utilizador e o seu direito de informação relativamente a este tipo de publicidade.

Ambas as cartas procuram reforçar regras quanto ao tratamento de dados, de modo a que o utilizador de *internet* tenham um efectivo controlo sobre os seus dados, só publicitando os dados que realmente querem.

Concluindo, apesar de não estar explícito na DP o direito dos titulares de dados ao apagamento definitivo dos seus dados, o direito a ser esquecido já era discutido e defendido como um direito que assistia ao titular dos dados para controlar o uso e divulgação dos seus dados.

5. Aplicação prática do direito a ser esquecido.

O regime do direito a ser esquecido proposto já foi explanado anteriormente, pelo que iremos analisar como esse regime se aplicará na prática.

[40] Disponível em: http://www.solocalgroup.com/sites/default/files/documents/Charte_publicite_ciblee_et_droit_des_internautes.pdf

A Autoridade Europeia de Protecção de Dados na sua opinião relativamente à comunicação " Uma abordagem global da protecção de dados pessoais na União Europeia" formulou o direito a ser esquecido como o direito que garante às pessoas que os seus dados pessoais são automaticamente eliminados após um período definido de tempo ou o seu uso é proibido[41]. Afirmou que " (…) o valor que este direito traz é o de não requerer esforços ou insistência do titular dos dados para ter os seus dados eliminados, pois isso deve ser feito de um modo objectivo e automático".[42](tradução livre)

Deste modo o direito a ser esquecido é encarado como privacidade por defeito, uma vez que é o responsável pelo tratamento que deve criar todos os mecanismos necessários para eliminar os dados quando já não são úteis para as finalidades para que foram recolhidos, quando o consentimento foi retirado ou o titular se opôs ao tratamento dos dados.

Viktor Mayer – Schönberger, um professor do Oxford Internet Institute, da Universidade de Oxford, dedicou-se ao estudo da privacidade na Internet, entre outros temas. No seu trabalho "Delete: The virtue os forgetting in the digital age", propôs a indexação de uma data de validade aos dados que são recolhidos e tratados, para que fossem eliminados nessa data automaticamente.

Para aplicar uma data de validade aos dados pessoais tratados, a mesma tinha que ser colocada pelo responsável pelo tratamento ou pelo próprio titular dos dados, quando consente no tratamento dos dados. Mas isso implica que o titular dos dados tenha que colocar uma data de validade em todos os dados que divulga, podendo tornar-se incómodo e desincentivar a aplicação. No caso de ser o responsável pelo tratamento a determinar a data de validade, tal implicaria uma reformulação do software subjacente ao funcionamento da recolha e tratamento dos dados e fiscalização do cumprimento da eliminação.

[41] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS PESSOAIS, Opinião de 14 de Janeiro de 2011, parágrafo 88.
[42] Idem, Ibidem parágrafo 89.

No regime proposto os dados são eliminados através do pedido do titular dos dados. Isso mesmo se comprova com o enquadramento sistemático do direito a ser esquecido e ao apagamento, que está incluído no Capítulo III da P.REg sobre Direitos do Titular dos Dados. Logo sendo um direito subjectivo do titular dos dados significa que este tem o direito e o poder de o exercer contra o responsável pelo tratamento.

A P.Reg determina a criação deste direito mas não especifica o método a adoptar pelos responsáveis pelo tratamento para apagar os dados pessoais. Assim quando o titular dos dados exercer o seu direito a ser esquecido, como se efectuará o apagamento dos dados?

A Agência da União Europeia para a Rede e Segurança da Informação (*European Union Agency for Network and Information Security* – ENISA) formulou três formas de interpretar e aplicar o direito a ser esquecido e ao apagamento. A primeira, de aplicação mais restrita, consiste em eliminar todas as cópias dos dados de forma a não serem recuperados por nenhum software. A segunda forma de aplicar este direito seria encriptar os dados pessoais e permitir apenas a pessoas autorizadas o acesso aos dados. Todavia desta forma a informação torna-se indisponível para a maioria das pessoas, mas continua acessível mesmo que a uma minoria. A terceira forma é retirar dos índices das bases de dados e das páginas de resultados dos motores de pesquisa a hiperligação às informações, reduzindo desta forma a divulgação[43].

Se a primeira surge como a mais fidedigna face ao direito em causa, por eliminar todas as cópias da informação, a sua aplicação prática é difícil. Isto porque, a eliminação de informações pessoais na fonte original não implica que todas as cópias da informação sejam eliminadas, pois é difícil localizar todas as cópias. Por exemplo, uma pessoa que pede ao editor de uma página Web para eliminar os seus dados pessoais. Mesmo que ele os elimine, isso não significa que esses dados pessoais tenham sido eliminados, porque qualquer pessoa que tenha tido acesso à informação enquanto esta esteve disponível pode ter copiado e armazenado. Além disso mesmo após a eliminação da informação, ela continuará acessível aos utilizadores da internet porque só quando o motor de

[43] BACKES, Michael; DRUSCHEL, Peter; TIRTEA, Rodica, *The right to be forgotten – between expectations and practice*, Enisa – European Network and Information Security Agency, Novembro, 2012, pág. 7. Disponível em http://www.enisa.europa.eu/activities/identity-and_trust/library/deliverables/the-right-to-be-forgotten.

pesquisa actualizar o conteúdo das páginas *Web* que tem em memória *cache* é que a página será disponibilizada sem os dados eliminados. Coloca-se ainda o problema da autoridade ou jurisdição de uma pessoa ou entidade para eliminar todas as cópias da informação, uma vez que as cópias podem estar espalhadas por vários países.

A segunda já tem uma margem de aplicabilidade maior face à anterior. No entanto se o que justificou a criação deste direito foi permitir aos utilizadores da internet obterem um recomeço na internet, através da eliminação de dados que considerem ser desnecessária a seu divulgação, o facto de a informação ainda ser acessível a algumas pessoas, não concretiza plenamente o fundamento daquele direito. Está patente, tal como na primeira interpretação, a dificuldade do titular dos dados localizar todas as cópias dos dados, pois se é difícil localizar todas as cópias para as eliminar, também é difícil localizá-las para proceder à encriptação. Assim, tal como na primeira interpretação, existe o risco de nem todas as cópias serem encriptadas.

A terceira interpretação implicaria que os dados continuassem acessíveis na internet mas os motores de pesquisa e índices das bases de dados não apresentariam os dados. Apesar de ser a interpretação com uma aplicação prática maior, apenas se reduziria divulgação da informação, limitando-a à fonte original dos dados. Mas os dados continuam disponíveis na internet, podendo ser acedidos pelos utilizadores que conheçam a fonte original dos dados. Logo não existiria uma eliminação dos dados.

Concluindo, o modo como o responsável pelo tratamento cumprirá este direito a ser esquecido ainda necessita de ser clarificado, contudo a eliminação dos dados parece ser a forma mais correcta de cumprir este direito.

6. Críticas ao direito a ser esquecido

Comparando a directiva 95/46/CE e a Proposta de Regulamento verifica-se que o direito ao apagamento e ao bloqueio dos dados previsto no artigo 12º alínea b) da directiva, é revogado na proposta. O direito de acesso regulado no artigo 15º da Proposta de

Regulamento já não prevê o direito ao apagamento e ao bloqueio de dados nos moldes previsto no artigo 12º alínea b) da directiva.

No entanto, prevê que o responsável pelo tratamento deve informar o titular dos dados da "existência do direito de solicitar ao responsável pelo tratamento a rectificação ou o apagamento de dados pessoais que lhe digam respeito, ou de se opor ao tratamento desses dados pessoais" (artigo 15º n.º1 al. e) da PReg). O direito ao apagamento aqui referido será o direito a ser esquecido e ao apagamento.

O direito a ser esquecido é o desenvolvimento do direito ao apagamento previsto na directiva[44]. Contudo este direito não parece adicionar concretamente um reforço do controlo dos dados pelos seus titulares, em comparação do regime da directiva. O apagamento dos dados continua a ser por iniciativa do titular dos dados, implicando que ele tenha conhecimento dos casos em que os seus dados estão a ser tratados e que conheça o responsável pelo tratamento para lhe requerer o apagamento.

Por fim, o direito a ser esquecido tem sido interpretado como uma forma de censura. O facto de a pessoa poder eliminar informações sobre si pode tornar a informação disponível ao público incompleta e descontextualizada, o que limitaria o direito de acesso à informação e a liberdade de expressão. Por exemplo, António divulga na sua página de uma rede social um comentário sobre várias pessoas. Uma dessas pessoas pode requerer a eliminação desse comentário, mas António quer manter o comentário. Dever-se-á eliminar o comentário ou mantê-lo, respeitando a liberdade de expressão?

Nestes casos, uma vez que estamos perante uma colisão de direitos, será necessário o Tribunal analisar o caso concreto e decidir qual o direito que prevalece.

[44] Proposta de regulamento do parlamento europeu e do conselho – COM (2012) 11 Final, página 9.

IV. Conclusões

Chegados ao fim da nossa exposição, cabe agora tecer algumas considerações a jeito de conclusões, sobre o tema tratado.

Podemos concluir que o titular dos dados está sujeito a tratamento dos seus dados em várias situações, mormente na Internet. Apesar de o fluxo de dados tratados na Internet não incluir apenas dados pessoais, o que é certo é que existem dados pessoais tratados através da *Internet*, por isso as entidades que realizem esses tratamento de dados são responsáveis pelo tratamento e por isso sujeitas a princípios e regras reguladoras do tratamento de dados, procurando evitar o uso abusivo desses dados.

Todos os tratamentos de dados pessoais realizados na Internet estão sujeitos à aplicação da directiva 95/46/CE, sendo que no caso específico do tratamento de dados pessoais realizado por prestadores de serviços de comunicações electrónicas, para além de cumprir as disposições da directiva 95/46/CE relativas a matérias de carácter geral sobre o tratamento de dados, também estão sujeito à aplicação da directiva 2002/58/CE, sobre tratamento de dados obtidos no âmbito da sua actividade.

Dada a evolução tecnológica crescente e as ameaças à privacidade do titular dos dados, consideramos que a consagração do direito a ser esquecido é de congratular, dada a necessidade de reforçar o controlo do titular dos dados sobre os seus dados.

Há, contudo, de verificar se o regime proposto vai efectivamente possibilitar um controlo pelo titular dos dados.

O Tribunal de Justiça da União Europeia, no acórdão C-131/12, já considerou que à luz da directiva 95/46/CE o titular dos dados tem direito a que os seus dados sejam suprimidos ao acesso do grande público, sem que para isso a publicação dos dados seja prejudicial ao titular. A supressão dos dados surge como garantia do direito ao respeito pela vida privada e direito à protecção de dados pessoais do titular dos dados.

O direito a ser esquecido é considerado uma inovação do regulamento proposto, pelo que se espera que comporte uma alteração ao regime dos direitos dos titulares de dados.

Da leitura do regime proposto parece, no entanto, que o direito a ser esquecido é uma clarificação e melhoramento do direito ao apagamento de dados previsto no artigo 12º al.b) da directiva 95/46/CE, uma vez que se limitam as situações em que o titular dos dados pode requerer o apagamento dos seus dados, pressupondo que o titular dos dados tem conhecimento sobre os vários tratamentos de dados a que é sujeito.

Cabe guardar pela discussão do Regulamento proposto e a sua, possível, adopção, para sabermos como os tribunais vão interpretar e aplicar o novo direito a ser esquecido.

Por fim, referir que a aplicação prática do direito a ser esquecido levanta dúvidas ao nível técnico, que necessitam ser esclarecidas pelo legislador comunitário.

V. Bibliografia

Monografias

- Castro, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais,* Almedina, Coimbra, Fevereiro 2005.
- Canotilho, Gomes; Moreira, Vital, *A Constituição da República Portuguesa Anotada*, Vol. I, 4ª Edição, Coimbra, Coimbra Editora.
- JÜRGEN SCHWABE, *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão,* Tradução Beatriz Hennig, Leonardo Martins,e outros, Konrad – Adenauer – Stiftung E.V., 2005.

Artigos

- AMBROSE, Meg Leta; AUSLOOS, Jef, "The right to be forgotten across the pond", Março, 2012. Disponível em http://p/apers.ssrn.com/sol3/papers.cfm?abstract_/id=2032325, data da consulta a 18/11/2013.

- AULOOS, Jef, "The right to be Forgotten'-Worth Remembering?". Disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1970392, data da consulta a 28/10/2013.

- BACKES, Michael; DRUSCHEL, Peter; TIRTEA, Rodica, *The right to be forgotten – between expectations and practice,* Enisa – European Network and Information Security Agency, Novembro, 2012. Disponível em http://www.enisa.europa.eu/activities/identity-and trust/library/deliverables/the-right-to-be-forgotten, data de consulta a 18/09/2013.

- BRANDEIS, Louis D., WARREN , Sameule D., "The Right to Privacy", Harvard Law Review, Vol. IV, n.º5, Dezembro 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm, data da consulta a 15/11/2013.

- CASTELLANO, Pere Simón, "The right to be forgotten under European Law: a Constitucional debate", Lex Electronica, vol. 16.1, 2012. Disponível em http://www.lex-electronica.org/docs/articles_300.pdf, data da consulta a 28/11/2013.

- CASTRO, Catarina Sarmento e, "O direito à autodeterminação a e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro". Disponível em: http://www.estig.ipbeja.pt/~ac_direito/CatarinaCastro.pdf, data da consulta a 01/03/2014.

- DE TERWANGNE, Cécile, "Privacidade n Internet y el derecho a ser olvidado / derecho al olvido", *Revista de internet, derecho y política*, n.º 13, fevereiro, 2012. Disponível em http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_esp, data de consulta a 02/12/2013.

- KUNER, Christopher, "Privacy, Security and Transparency: Challenges for data protection law in a new europe", *European Business Law Review,* volume 16, Issue 1, Klumer Law International, 2005, páginas 1 a 8.

- LOPES, J. de Seabra Lopes, "A Protecção da Privacidade e dos dados pessoais na sociedade da informação: tendências e desafios numa sociedade em transição", in *Estudos dedicados ao Prof. Doutor Mário Júlio Brito de Almeida Costa*, Universidade Católica Editora, Lisboa, 2002, páginas 779 a 807.

- ROSEN, Jeffrey, "The right to be forgotten", Stanford Law Review, SLR Online, 13 Fevereiro, 2012. Disponível em http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten, data da consulta a 15/11/2013.

Outros Documentos

- Opinião da Autoridade Europeia de Protecção de Dados sobre a comunicação da comissão ao Parlamento Europeu, ao Conselho, do Comité económico e social e Comité das regiões – " A comprehensive approach on personal data protection in the european union", 14 de Janeiro de 2011, parágrafos 83 a 91. Disponível em: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf. Data da consulta: 01/11/2013.

- Documento de Trabalho do Grupo do Artigo 29º, "Privacidade na Internet – Uma abordagem integrada da EU no domínio da protecção de dados em linha". Aprovado em 21 de Novembro de 2000. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_pt.pdf#h2-15. Data da consulta: 01/03/2014

- Agência Espanhola de Protecção de Dados, "Guía sobre el uso de las cookies". Disponível em: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php. Data da Consulta: 01/05/2014

- "Attitudes on Data Protection and Electronic Identity in the European Union", Eurobarometer Especial 359, publicado em Junho de 2011. Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. Data de acesso: 24 de Abril de 2014.

- Agência Espanhola de Protecção de Dados, Procedimiento n.º PS/00321/2012. Disponível em: http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php. Data da Consulta: 01/05/2014

- Grupo de Trabalho do artigo 29º, Opinião 01/2012 sobre as propostas de reforma do regime de protecção de dados pessoais, de 23/ 03/2012. Disponível em:

http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/index_en.htm, data da consulta: 21/01/2014.

- CNIL, 30e Rapport d' activité 2009, Disponível em: http://www.cnil.fr/documentation/rapports-dactivite/. Data da Consulta: 20/04/2013.

- Preposition de loi visant à mieux garantir le droit à la vie privée à l'heure e du númerique, submetida por Yves Détraigne e Anne – Marie Escoffier, apresentada a 6 de novembro de 2009. Disponível em : http://www.senat.fr/leg/ppl09-093.html. Data da Consulta: 01/03/2014

- *Charte du droit a l'oubli dans les sites collaboratifs et les moteurs de recherche.* De 13 de Outubro de 2010, disponível em : http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf. Data da Consulta: 01/03/2014

- *Charte sur la publicite ciblee et la protection des internautes, de 30 de Setembro* de 2010, disponível em :http://www.solocalgroup.com/sites/default/files/documents/Charte_publicite_ciblee_et_droit_des_internautes.pdf. Data da Consulta : 01/03/2014

Jurisprudência do Tribunal de Justiça da União Europeia:

- Processo C-101/01, de 6 de Novembro de 2003. Disponível em: http://eur-lex.europa.eu/legalcontent/PT/TXT/?qid=1400069636627&uri=CELEX:62001CJ0101. Data de consulta: 15 de Fevereiro de 2014.

- Processo C-131/12:
    - Acórdão de 13 de Maio de 2014, disponível em : http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62012CJ0131. Data da Consulta: 13/05/2014.

- Conclusões do Advogado – Geral: http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=410516. Data da Consulta: 20/04/2013